Making the Case for Elliptic Curves in DNSSEC

an analysis of the impact of switching to ECC based on current DNSSEC deployments in .com, .net and .org

UNIVERSITY OF TWENTE
Introduction

- DNSSEC deployment has taken off, but there are still operational issues
  - Fragmentation
  - Amplification
  - Complex key management
- Root cause of many of these problems: use of RSA
- ECDSA standardised in RFC 6605 (2012), but still sees very little use (but is discussed a lot!)
Fragmentation

• Well known problem; up to 10% of resolvers may not be able to receive fragmented responses*

• Solutions available:
  • Configure **minimal responses**
  • Better fallback behaviour in resolver software
  • Stricter phrasing of RFC 6891 (EDNS0)

Fragmentation

- Setting **minimal responses** pays off:

![Graph showing average response size](image1)

- But fragmentation still occurs!

![Graph showing fragmentation IPv4/IPv6](image2)
Amplification

- DNSSEC is a potent amplifier*

Amplification

- While ANY could be suppressed, DNSKEY cannot!
Root cause: RSA

- RSA keys are large
  - 1024-bit —> 128 byte signatures, ±132 bytes DNSKEY records
  - 2048-bit —> 256 byte signatures, ±260 bytes DNSKEY records
- Also: striking a balance between signature size and key strength means RSA prevents a switch to simpler key management mechanisms*

*don’t have time to explain in detail, see paper
ECC to the rescue

• ECC has much smaller keys and signatures with equivalent or better key strength
  
  • ECC with 256-bit group \( \approx \) RSA 3072-bit

• ECDSA P-256 and P-384 are standardised for use in DNSSEC in RFC 6605 (2012)
  
  • Used very little in practice, 99.99% of .com, .net and .org use RSA

  • But there is a lot of buzz around it (CloudFlare!)

• EdDSA based schemes have draft RFCs (Ondřej Surý)
Measuring ECC impact

- We performed a measurement study to quantify the impact of switching to ECC on fragmentation and amplification.

- Study looks at all signed .com, .net and .org domains.

- Studies ECC scenarios:

<table>
<thead>
<tr>
<th>implementation choice</th>
<th>ecdsa384</th>
<th>ecdsa256</th>
<th>ecdsa384csk</th>
<th>ecdsa256csk</th>
<th>eddsasplit</th>
<th>eddsacsk</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDSA vs. EdDSA Curve</td>
<td>ECDSA</td>
<td>ECDSA</td>
<td>ECDSA</td>
<td>ECDSA</td>
<td>EdDSA</td>
<td>EdDSA</td>
</tr>
<tr>
<td></td>
<td>P-384</td>
<td>P-256</td>
<td>P-384</td>
<td>P-256</td>
<td>Ed25519</td>
<td>Ed25519</td>
</tr>
<tr>
<td>KSK/ZSK vs. CSK</td>
<td>KSK/ZSK</td>
<td>KSK/ZSK</td>
<td>CSK</td>
<td>CSK</td>
<td>KSK/ZSK</td>
<td>CSK</td>
</tr>
<tr>
<td>most conservative</td>
<td>←</td>
<td></td>
<td>←</td>
<td>←</td>
<td>↑</td>
<td>→</td>
</tr>
<tr>
<td>most beneficial</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Impact on fragmentation

- DNSKEY response sizes dramatically reduced:

![Graph showing impact on fragmentation]
Impact on amplification

- ANY amplification dampened significantly:

![Graph showing the impact of amplification on different domains. The x-axis represents the amplification factor [bin=0.1], and the y-axis represents the percentage of domains. The graph compares the current situation with ecdsa256, ecdsa256csk, and eddsacsk, showing a significant dampening effect in the theoretical maximum amplification of regular DNS.]
Impact on amplification

- DNSKEY amplification practically solved:

Graph showing the theoretical maximum amplification of regular DNS and the amplification factors for various DNS key types (original, ecdsa384, ecdsa256, ecdsa256csk, eddsacsk). The x-axis represents the amplification factor (bin=0.1), and the y-axis represents the percentage of domains.
Back to 512-byte DNS?

- A and AAAA responses fit in classic DNS!

![Graph showing the percentage of domains with A and AAAA queries based on response size.](graph)

- A queries: Full line
- AAAA queries: Dashed line

**X-axis:** response size [ecdsa256 with minimal responses]

**Y-axis:** percentage of domains
Conclusions

- Switching to ECC is highly beneficial and tackles major issues in DNSSEC

- Combined with simpler key management it could even bring “classic” 512-byte DNS back into scope

- Impact on resolvers is uncertain! ECC validation speeds are up to an order of magnitude slower than RSA

- Improvements are being made (e.g. OpenSSL)

- We are working on quantifying the impact of this
Further reading and future work

- For an in-depth discussion of this material, see our CCR paper*

- We are working on quantifying the impact of switching to ECC on resolvers (M.Sc. project finishing tomorrow, Oct. 22), expect another paper soon

Thank you for your attention!

Questions?

nl.linkedin.com/in/rolandvanrijswijk
@reseauxsansfil
roland.vanrijswijk@surfnet.nl
r.m.vanrijswijk@utwente.nl